System Libraries And Utilities - Old Protection Mechanism

⚠ Natural Security provides two mechanisms to control the use of Natural utilities: the old mechanism is described in this section, the new mechanism is described in the section Protecting Natural Utilities.
It is strongly recommended that the new mechanism be used, as it provides more efficient protection of utility functions. The old mechanism will be removed with one of the next releases of Natural Security.

This section describes the considerations that apply to the protection by Natural Security of the following utilities/commands:

- NATUNLD/NATLOAD under Natural Security
- SYSERR under Natural Security
- SYSMAIN under Natural Security
- SCAN Command under Natural Security

NATUNLD/NATLOAD under Natural Security

Restricting the Use of NATUNLD/NATLOAD Itself

The availability of the Natural unloading and loading utilities NATUNLD and NATLOAD as such cannot be controlled by Natural Security. However, you can control the use of these utilities for loading objects from and into specific libraries, as described in the following section.

Unloading/Loading of Libraries/Private Libraries

The permission to load objects from and into libraries and private libraries with NATLOAD and NATUNLD respectively is controlled by the setting of the "Utilities" option in the security profile of a library/private library.

Unloading/Loading Permission for Libraries

In a library’s security profile you may specify the "Utilities" option. This option may take one of the following values:

N	**No protection** - The contents of the library may be unloaded/loaded by anybody.
O	**Permission for Owners** - Only the owners of the library unload/load its contents; if no owner is specified, any user of type ADMINISTRATOR may do so.
P	**Permission under Protection rules** - The People/Terminal protection of the library applies: only users who may use the library - and only under the conditions under which they may use it - may unload/load its contents.

Unloading/Loading Permission for Private Libraries

Every user is allowed to unload/load the contents of his/her own private library.

Moreover, you may specify the "Utilities" option in the private library’s security profile. This option may take one of the following values:

N	**No protection** - The contents of the private library may be unloaded/loaded by anybody.
O	**Permission for Owners** - In addition to the user him-/herself, only the owners of the user's security profile may unload/load the private library's contents; if no owner is specified, any user of type ADMINISTRATOR may do so.
P	**Password protection** - A user may unload/load the contents of another user's private library only after entering that other user's password on a countersignature screen provided for that purpose.

SYSERR under Natural Security

The Natural error message maintenance utility SYSERR may also be defined and its use controlled by Natural Security.

Note:
Under Natural Security, the online use of the SYSERR program ERRULDUS for the unloading of messages on mainframe computers is only available to users of type ADMINISTRATOR (regardless of the setting the "Utilities" option described below).

Restricting the Use of SYSERR Itself

As far as defining and protecting is concerned, you may treat SYSERR like any other library.

As for the use of SYSERR itself, the same rules apply as for any other library defined under Natural Security; that is, if SYSERR is people-protected and/or terminal-protected, any user who is to use SYSERR must be linked accordingly. In other words, a user must be able to log on to SYSERR in order to use it.

Message Maintenance in Libraries/Private Libraries

The permission for maintaining with SYSERR library-specific error messages (user messages) in libraries and private libraries is controlled by the setting of the "Utilities" option (see General Options in the section Library Maintenance) in the security profile of a library/private library.

Maintenance Permission for Libraries

In a library's security profile you may specify the "Utilities" option. This option may take one of the following values:

N	**No protection** - The library's error messages may be maintained in SYSERR by anybody.
O	**Permission for Owners** - Only the owners of the library may maintain its error messages with SYSERR; if no owner is specified, any user of type ADMINISTRATOR may do so.
P	**Permission under Protection rules** - The People/Terminal protection of the library applies: only users who may use the library - and only under the conditions under which they may use it - may maintain its error messages with SYSERR.

Maintenance Permission for Private Libraries

Every user is allowed to maintain the error messages in his/her own private library.

Moreover, you may specify the "Utilities" option in the private library's security profile. This option may take one of the following values:

N	**No protection** - The private library’s error messages may be maintained in SYSERR by anybody.
O	**Permission for Owners** - In addition to the user him-/herself, only the owners of the user’s security profile may maintain the private library’s error messages; if no owner is specified, any user of type ADMINISTRATOR may do so.
P	**Password protection** - A user may maintain error messages in another user’s private library only after entering that other user’s password on a countersignature screen provided for that purpose.

SYSMAIN under Natural Security

The Natural object maintenance utility SYSMAIN may also be defined and its use controlled by Natural Security.

Please note that the SYSMAIN utility is not identical on all platforms.

Restricting the Use of SYSMAIN Itself

As far as defining and protecting is concerned, you may treat SYSMAIN like any other library.

As for the use of SYSMAIN itself, the same rules apply as for any other library defined under Natural Security; that is, if SYSMAIN is people-protected and/or terminal-protected, any user who is to use SYSMAIN must be linked accordingly. In other words, a user must be able to log on to SYSMAIN in order to use it.

On mainframes, you may also restrict the use of SYSMAIN, i.e. the availability of functions provided by SYSMAIN, by disallowing modules.

SYSMAIN Maintenance of Libraries/Private Libraries

The permission for SYSMAIN maintenance of libraries and private libraries is controlled by the setting of the "Utilities" option (see General Options in the section Library Maintenance) in the security profile of a library/private library.

Maintenance Permission for Libraries

In a library’s security profile you may specify the "Utilities" option. This option may take one of the following values:

N	**No protection** - The library may be maintained with SYSMAIN by anybody.
O	**Permission for Owners** - Only the owners of the library may maintain it with SYSMAIN; if no owner is specified, any user of type ADMINISTRATOR may do so.
P	**Permission under Protection rules** - The People/Terminal protection of the library applies: only users who may use the library - and only under the conditions under which they may use it - may maintain it with SYSMAIN.

Batch Processing

When using SYSMAIN in batch mode, only those libraries for which no countersignature from a co-owner is required for maintenance permission can be maintained (as countersignatures are not allowed in batch mode).

Maintenance Permission for Private Libraries

Every user is allowed to maintain his/her own private library.

Moreover, you may specify the "Utilities" option in the private library’s security profile. This option may take one of the following values:

N	**No protection** - The private library may be maintained with SYSMAIN by anybody.
O	**Permission for Owners** - In addition to the user him-/herself, only the owners of the user’s security profile may maintain the private library with SYSMAIN; if no owner is specified, any user of type ADMINISTRATOR may do so.
P	**Password protection** - A user may maintain another user’s private library only after entering that other user’s password on a countersignature screen provided for that purpose.

Batch Processing

When using SYSMAIN in batch mode, only those private libraries for which no countersignature from a co-owner is required for maintenance permission can be maintained (as countersignatures are not allowed in batch mode). If the "Utilities" option is set to "P", no user may maintain another user’s private library in batch mode (as no password can be entered in batch mode).

SYSMAIN Functions LIST and FIND

When using the SYSMAIN functions LIST and FIND, a user will obtain a list of only those libraries/private libraries which he/she is allowed to maintain with SYSMAIN.

SCAN Command under Natural Security

The use of the Natural system command SCAN may also be controlled for each library (or private library) by Natural Security.

You can either disallow the SCAN command altogether for a library via the "Command Restrictions" option in the library security profile, or you can control its use via the "Utilities" option in the library security profile.

- If you mark the SCAN command with "Y" on the Command Restrictions screen of a library profile, the use of the SCAN command within that library is controlled by the setting of the "Utilities" option in the library profile, as explained below.
- If you mark the SCAN command with "N" on the Command Restrictions screen of a library profile, the SCAN command cannot be used within that library (regardless of the setting of the "Utilities" option).

Where and how both options are set is described in section Library Maintenance under General Options and Command Restrictions respectively.

SCAN Permission for Libraries

In a library’s security profile you may specify the "Utilities" option. This option may take one of the following values:

N	**No protection** - The SCAN command may be used in the library by anybody.
O	**Permission for Owners** - Only the owners of the library may use the SCAN command; if no owner is specified, any user of type ADMINISTRATOR may use it.
P	**Permission under Protection rules** - The People/Terminal protection of the library applies: only users who may use the library - and only under the conditions under which they may use it - may use the SCAN command.

Batch Processing

When using the SCAN command in batch mode, it can only be used for those libraries for which no countersignature from a co-owner is required for maintenance permission (as countersignatures are not allowed in batch mode).

SCAN Permission for Private Libraries

Every user is allowed to use the SCAN command in his/her own private library.

Moreover, you may specify the "Utilities" option in the private library’s security profile. This option may take one of the following values:

N	**No protection** - The SCAN command may be used in the private library by anybody.
O	**Permission for Owners** - In addition to the user him-/herself, only the owners of the user’s security profile use the SCAN command; if no owner is specified, any user of type ADMINISTRATOR may use it.
P	**Password protection** - A user may use the SCAN command in another user’s private library only after entering that other user’s password on a countersignature screen provided for that purpose.

Batch Processing

When using the SCAN command in batch mode, it can only be used for those private libraries for which no countersignature from a co-owner is required for maintenance permission (as countersignatures are not allowed in batch mode). If the "Utilities" option is set to "P", no user may use the SCAN command in another user’s private library in batch mode (as no password can be entered in batch mode).